

Voluntary Service System (VSS) Site Installation Guide

**Revision 2.4
August 22, 2003**

Department of Veterans Affairs
VHA System Design & Development (SD&D)
VistA Migration Service

Revision History

Documentation History

Date	Revision	Description	Author
March 18, 2003	1.0	Document issued as Part 2 of the <i>VSS Installation Guide</i> , under the title “Site Implementation Guide.” Contained information for local IRMs and Voluntary Services to use to: <ul style="list-style-type: none"> Set up and configure equipment and software required to run the VSS application Migrate local Voluntary data to the national database at the EMC. 	Mike Garvey, Ron DiMiceli, Cathi Graves, Lloyd Hurt, and Jim Alexander.
May 2, 2003	2.0	Material issued as standalone document under the title, <i>Site Installation Guide</i> . Incorporated minor changes, especially in the section “Setting Up the Auto-login kiosk.”	Jim Alexander, Mike Garvey
May 8, 2003	2.1	Minor changes to Revision and TOC sections.	Jim Alexander
May 16, 2003	2.2	Addition to the “IRM Data Transmission Instructions” in the “Data Migration Instructions” section.	Jim Alexander, Ron DiMicelli
May 21, 2003	2.3	Minor change to “Auto-Login Kiosk Setup Instructions” section.	Jim Alexander, Mike Garvey
August 22, 2003	2.4	Additional instructions to “Auto-Login Kiosk Setup Instructions” for MS Service Pack 4 installation.	Jim Alexander, Mike Garvey

Patch History

The history of VSS is included in the application Release Notes.

Revision History

Acknowledgements

The Voluntary Service System (VSS) team consists of the following personnel:

- VistA Migration Program Manager – Maureen Hoye
- Project Manager – Rebecca Byrd
- Developers – Mike Langley, Ron DiMiceli, and Rick Jones
- Requirements Analysts – Conrad Sweeting and Ken Bowers
- Database Administrators – Deborah Goff and Don Creaven
- System Administrator – Mike Garvey
- Build Master – Sachy Kulkarni
- Testers – Gary Davisson and Rob Duarte
- Technical Writers – Jim Alexander and Phylis Carlin
- Training Coordinator – Monique Allen

Acknowledgements

Contents

Revision History	iii
Documentation History	iii
Patch History	iii
Acknowledgements	v
Contents	vii
Introduction	1
Audience and Scope	1
Contents	1
Implementation Roles	1
Implementation Steps for IRM and Voluntary	3
IRM	3
Voluntary Staff	4
System Requirements	9
Workstation Hardware	9
Workstation Software	9
Meal Ticket Printer	9
Thin Client	9
Browser Setup Instructions	11
Auto-Login Kiosk Setup Instructions	15
Overview	15
Kiosk Setup Steps	15
Troubleshooting	26
Installing Windows Patches	27
Data Migration Instructions	29
Data Cleansing	29
IRM Installation Instructions	29
Voluntary Data Cleansing Instructions	30
1. Prepare for Transition to VSS	31
2. Validate Existing Data	32
3. Print Data Validation Results	32
4. Correct Data Errors	33

Contents

5. Repeat Validation and Correction (steps 2-4)	34
Data Transmission	35
Two Transmissions: Test and Production	35
IRM Data Transmission Instructions	35
Voluntary Data Transmission Instructions	36
Appendix A: VSS RASIC Chart	38
Appendix B: VSS Implementation Diagram	40
Appendix C: Auto-Login Policy Definitions	42

Introduction

Audience and Scope

This document is for the use of IRM and Voluntary Service groups at VHA sites during the implementation of the VSS application in 2003. It contains information for setting up equipment required by the VSS application and for migrating local Voluntary data to the national database at the EMC. This guide does not address the entire national implementation of VSS, only the preparation for and switchover to the new application at the Voluntary site level.

All of this material has been released previously as separate documents or bundled with information for other audiences. The purpose of this document is to put all the site implementation materials together in one place. The document contains all revisions that have been made to previously released information.

Contents

This guide includes the following material:

- Checklists of IRM and Voluntary of implementation tasks
- System requirements for Voluntary PCs, auto-login kiosks, meal-ticket printers
- Browser setup instructions
- Kiosk setup instructions
- Instructions for running the two data migration patches.

The site IRM contacts will need to refer to all of these materials to ready the sites for their go-live dates and to migrate data at the scheduled time from the site to the EMC. All Voluntary and IRM staff should refer the *Site Implementation Checklist* section to understand the implementation process at the site level. *Appendix B: VSS Implementation Diagram* presents most of the same information in a more condensed form.

The IRM should refer to the *System Requirements*, *Browser Setup Instructions*, and *Kiosk Setup Instructions* two or three weeks before migration to set up equipment and software required by the new system. The IRM should refer to the *Data Migration Instructions* section for the patch installation procedure. The Voluntary POC should read this section to understand the process for cleaning up the data and then transmitting the clean data to the EMC immediately prior to using the new system.

Implementation Roles

It is the role of System Implementation (SI) to plan and coordinate the nationwide rollout of VSS. SI will work closely with the following groups to provide scheduling, training,

Introduction

technical support, and go-ahead certification during various phases of the VSS implementation:

- National Vista Support (NVS)
- National Training Education Office (NTEO)
- Enterprise Management Center (EMC)
- Central Office of Voluntary Services (CO)
- Local Voluntary Services
- Local Information Resource Management (IRM) groups

Each Voluntary Chiefs will assign a POC for SI to coordinate with during implementation. The POC will be responsible for the following:

- Assist the IRM with the equipment survey and coordinate equipment setup
- Run the two data migration patches
- Function as the VSS user administrator as soon as the site is created by the EMC.

See *Appendix A: VSS Basic Chart* for more information about the roles and levels of responsibilities for the various groups involved with the development and implementation of the VSS application.

The POCs for the SI team are:

- Rebecca Byrd, National Project Manager (510-768-6853)
- Lloyd Hurt, SI Project Coordinator (360-335-8339)
- Chuck Krochmal, SI Project Coordinator (734-954-0641)
- John Marple, SI Implementation Manager (410-569-1423)

Implementation Steps for IRM and Voluntary

This section lists the steps that the IRM and Voluntary Services will need to take to implement the VSS system at a VHA facility. This section should serve as an overview and checklist. Some of the steps listed here refer to other parts of this document, where the information is described in much greater detail.

The implementation steps summarized in the text are divided into two sections, one for the IRM, and one for Voluntary. Although IRM and Voluntary Services have different responsibilities during the implementation process, they must coordinate and communicate carefully for the equipment upgrade, kiosk installation, data cleansing, and data migration to be successful.

It should be stressed that during the Alpha and Beta implementations, the most problematic step was the installation of the Auto-Login Kiosks. It is crucial to the success of site implementation, therefore, to set up, test, troubleshoot, and instruct staff on the use of auto-login kiosks well in advance of data migration. It is highly recommended that an IRM resource be reserved for two full days during the two weeks prior to data migration to troubleshoot the auto-login/meal-ticket printer.

See *Appendix B* for a diagram of the VSS Implementation Process, which shows the major events and flow in the implementation process.

IRM

Coordinate with Voluntary. Contact Voluntary Services Chief to discuss tasks, schedules, and the Voluntary staff who will support the IRM during implementation.

Equipment Survey. Examine Voluntary equipment survey sheet and determine the following:

- Which currently used equipment does not meet VSS system requirements (see the section *System Requirements*.)
- Which login locations have dumb terminals. You will need to replace these with PCs.
- Remote login locations that will have to be locked down in kiosk mode.

Equipment Upgrade. Replace and upgrade equipment and software identified in step 1 for staff computers and volunteer auto-login stations.

Internet Access. Ensure that VSS staff who will be doing administrative work have internet access. They will need:

Implementation Steps

- Microsoft Internet Explorer 5.5 or higher, with SP2. (IE 6.0 is highly recommended)
- Internet access
- NT domain and username

Browser LAN Settings. Assist VSS administrator to change browser LAN settings on computers with Internet access. Ensure that the site has a trust relationship with VHAMASTER. (See *Setting Up Browsers*.)

Test Connectivity. Test Internet connectivity for each machine.

Set Up and Test Kiosks. Set up, test, and instruct staff on the use of auto-login kiosks. Reserve two full days of an IRM resource within the two weeks before data migration to troubleshoot and practice the auto-login/meal-ticket printer installation. **This step is the most crucial to the success of the VSS implementation.**

Verify the connection types needed for both the PC and the printer. Make sure you have the correct setup for your particular situation.

The IRM is required to test the kiosk prior to going live with VSS. If they encounter any problems, they will log a NOIS, and if NVS cannot resolve the issue, then the NOIS will have to be referred to a technical resource in SD&D. (See the section *Setting Up the Auto-Login Kiosk*.)

Data Cleansing. When notified by NVS, load Patches ABSV*4.0*31 and ABSV*4*33 for data cleansing. (See the section *Data Migration*.) Make sure that the appropriate person in Voluntary has been assigned responsibility for running the patch.

Data Transmission. The NVS will notify IRM that it is ready to receive data. It will send a password and an e-mail address where the data is to be sent. The IRM should then:

- Disable VistA log-in for volunteers
- Run Patch ABSV*4.0*32
- Once data has migrated, disable the options in VistA for VTK, to prevent loss of data.

(See the section *Data Migration Procedures*.)

Message from EMC. Receive message from EMC whether or not data has been received and entered into database. If there is a problem, the EMC will give instructions.

Voluntary Staff

Coordinate with IRM. Contact IRM to discuss tasks, schedules, and the Voluntary staff who will support the IRM during implementation.

Implementation Steps

Equipment Survey. A Voluntary service representative should use the SI survey sheet to make a list of the equipment and software used by VSS staff and by volunteers at login locations. Make special note of the following in the survey:

Locations where dumb terminals are used (the IRM will need to replace these)
Remote locations, away from office staff (the IRM will need to lock these down in “Kiosk mode”). Deliver and discuss the list with an IRM representative.

Security Agreements. Each staff person who will be using the VSS system should sign a security agreement, in coordination with both the facility ISO and the designated Voluntary Services VSS Site User Administrator. A typical site will have no more than five or six users needing access.

Browser LAN Settings. Change LAN settings on browsers. (See the section *Browser Setup*.) If Voluntary administrator does not have administrator access to do this, request that the IRM do this.

New Volunteer Kiosk Test. Enter a small number of new volunteers into the VTK system prior to migration and enter hours for them and print meal tickets using the new auto-login kiosks. These volunteers should be held back after orientation in order to participate in the test. The kiosks will be pointed to the EMC’s production database.

Send Kiosk and Printer Certification to SI. Send certification to SI Implementation Manager that auto-login kiosk and meal-ticket printer are working successfully.

Run Data Cleansing Patch. When the IRM notifies Voluntary that it has loaded it, run Patch ABSV*4.0*31 to clean the data. This will happen two weeks before the data migration. Run the patch, examine the report, correct the error, and rerun the patch. Run the patch as many times as necessary to eliminate all errors.

The first portion of this patch provides facility demographic data that will be used to create and populate the EMC database. This information should be sent to:

WAITING ON EMC SOLUTION.

Send Data Cleansing Certification to Implementation Manager. Send certification to SI Implementation Manager that data cleansing is complete and that data is ready to be migrated. (SI will notify sites who their Implementation Manager is.)

Run Data Transmission Patch to Test Site. Two weeks before the actual data migration, SI will notify the site to run the second patch (ABSV*4.0*32) to transmit the local VTK database to the EMC *test* site. This is a rehearsal for the site, and may reveal any transmission or data problems ahead of time.

Print VTK Test Reports. The afternoon prior to transmitting data, run the following reports from the VistA system:

Implementation Steps

- Daily views for two volunteers
- Occasional Hours by Organization for two organizations
- Regular Scheduled Hours by Organization for two organizations.

Review Local Organization (900-999) and Service (800-899) Codes. Follow SIs instructions for printing a listing of these codes. If you do not have Fileman access, ask IRM to run the reports. If you do have duplicate or erroneous codes, ask IRM to log a NOIS to the National Vista Help Desk at 1-888-596-4357. **Do not delete any codes -- this will corrupt your database.**

VSS will automatically give you the next available number when entering a new service/organization code.

Manually Run the Transfer Time to Daily Time File. When you are ready to migrate the data, stop the auto-login. Manually run the Transfer Time to Daily Time File option located on the Auto-Login menu. Otherwise, volunteer hours may be lost. Check that the Daily Time File is up to date before Migration. The hours may need to be adjusted manually.

Roll Up Data. It is recommended that sites roll up their data from the Vista Transmission/Pre-transmission/Roll up menu option and print the listing. Do not transmit the data.

Coordinate Migration with Substations. Integrated sites should coordinate with substations to send their data separately during the migration. **Each site should run the patch for their data only.**

Actual Data Migration Patch to Production Site. On the implementation date SI will notify the site to run the second patch (ABSV*4.0*32) to transmit the local VTK database to the EMC via Outlook Messaging. SI and or VSS team will provide site with email address, notify EMC, and set up site in the production database.

Data Migration Error Correction. After running the data transmission patch, Voluntary Service will receive a listing from the EMC of any transmission errors. These errors should be corrected so that data can be sent again.

VSS Site Administration. The Site User Administrator should log on to the new VSS system and do the following:

1. Assign access roles to all Voluntary staff via User Management screens
2. Set site parameters (meals, price, language, etc.) on the Site Parameters screen.

Run Reports from New System. Run the following reports again, this time from new VSS system:

Implementation Steps

- Volunteer Daily Review
- Occasional Hours by Organization (use same organizations as before)
- Regular Scheduled Hours by Organization (use same organizations as before)

Compare the two sets – the data should be the same.

Auto-Login Test. If the data in report comparison in the preceding step is the same:

- Point the browser to the auto-login screen
- Test the auto-login program by having a couple of volunteers sign in.

Go Live. The VSS staff should start using the new system and report anything that does not work properly to SI.

Implementation Steps

System Requirements

Workstation Hardware

- Standard PC architecture, with Pentium 150MHz processor or greater
- 64 MB of RAM or greater
- 2 GB hard disk or greater, with a minimum of 60 MB of free space
- VGA or greater display adapter with color monitor
- Microsoft mouse or compatible pointing device
- A network interface card (NIC), with appropriate network transport software. Supported connection method and transport are TCP/IP and HTTP.

Workstation Software

- One of the following operating systems:
- MS Windows 2000
- Microsoft Service Pack 1 (necessary to run reports)
- Microsoft Internet Explorer 5.5 with Service Pack 2. (Internet Explorer 6.0 is highly recommended)
- Adobe Acrobat Reader Version 5.0
- Microsoft Office, with all service packs installed (necessary to run reports)
- Network transport software appropriate for the network interface card being used. The supported connection method and transport are TCP/IP and HTTP.

Meal Ticket Printer

- Star Micronics SP200 Dot Matrix Printer
- Serial cable using a D-sub9/MaleD-sub 25 connection
- Ink Cartridge

Thin Client

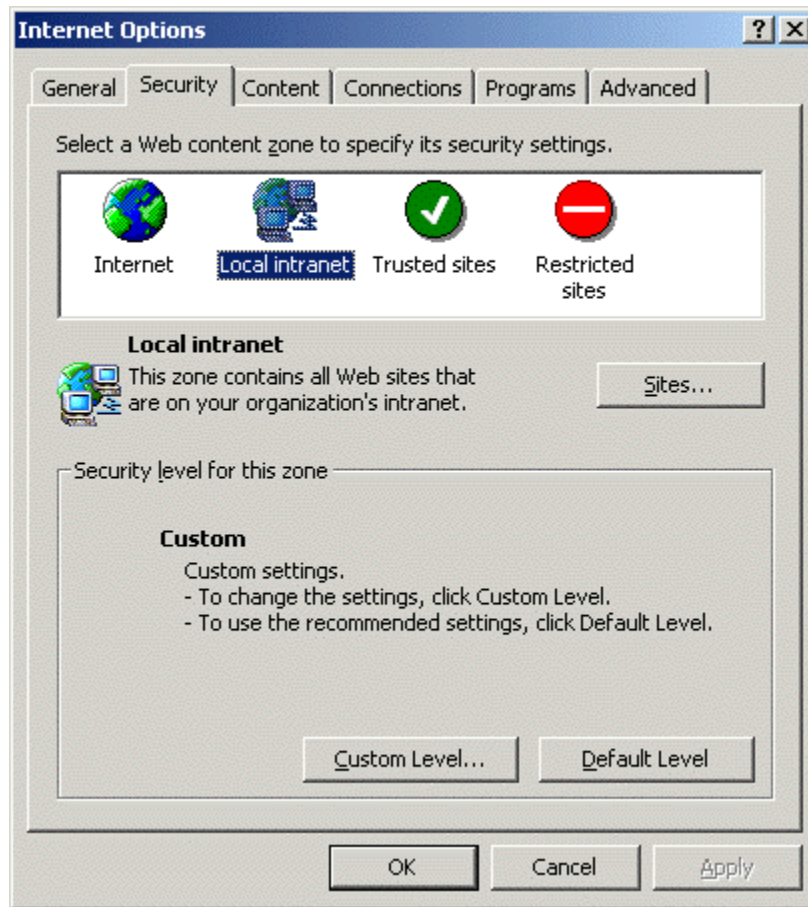
- If you want to set VSS up to run with Thin Client, please refer to the VSS web page at: <http://vista.med.va.gov/migration/vss> for instructions.

System Requirements

Browser Setup Instructions

To enable your copy of Internet Explorer (5.5. or 6.0) to identify "Local intranet" sites on the VA network, follow the steps below.

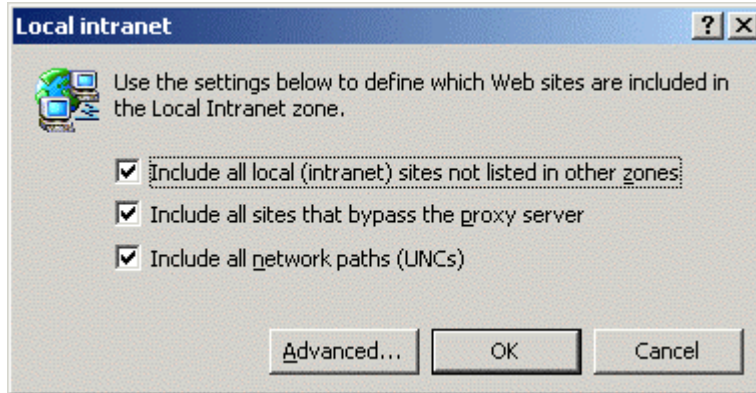
1. In IE, go to the Tools | Internet Options menu.
2. Choose the Security Tab:



3. In the Security tab, highlight "Local intranet" and click the Sites button.

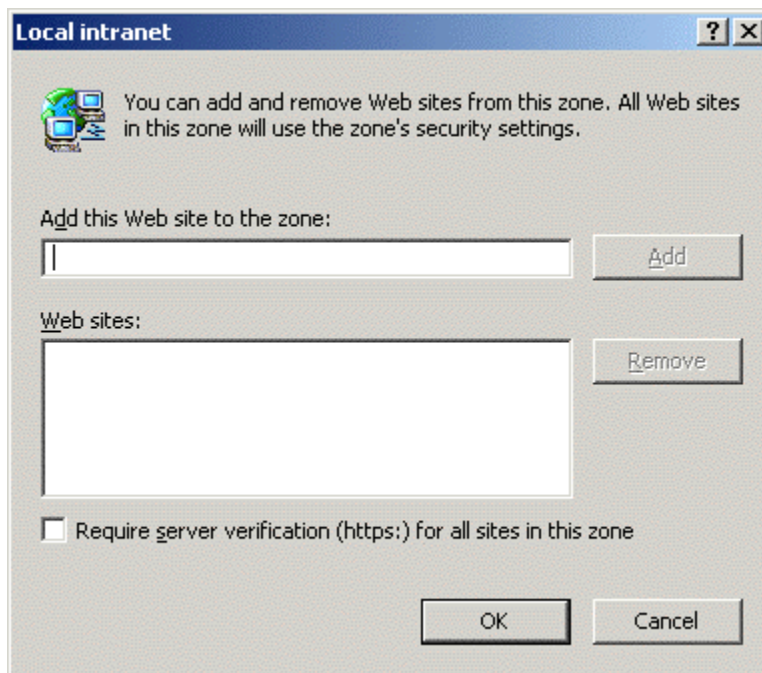
This brings up the "Local intranet" window:

Browser Setup Instructions



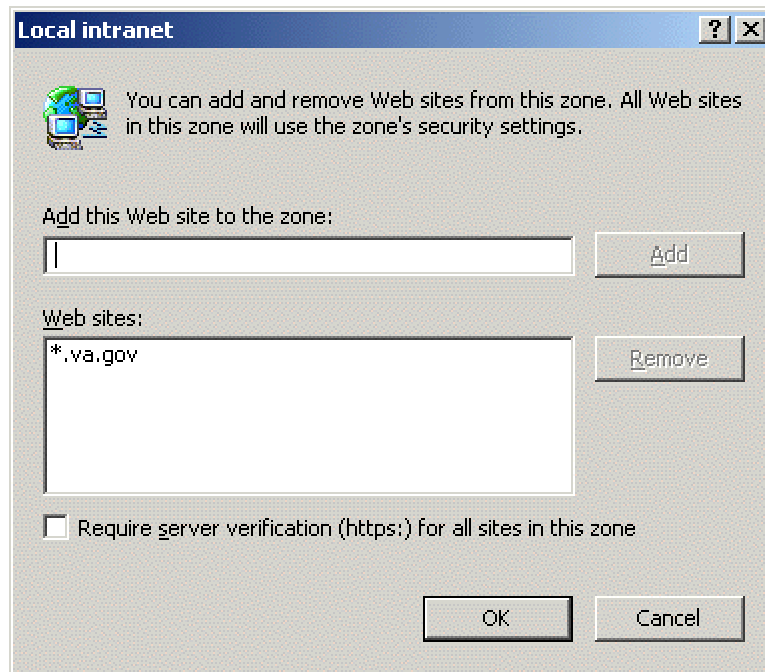
4. Click the Advanced button. (The settings for the three checkboxes in the "Local intranet" window are not important for this test.)

This brings up another "Local intranet" window. In this window, you can add web sites to the "Local intranet" zone:

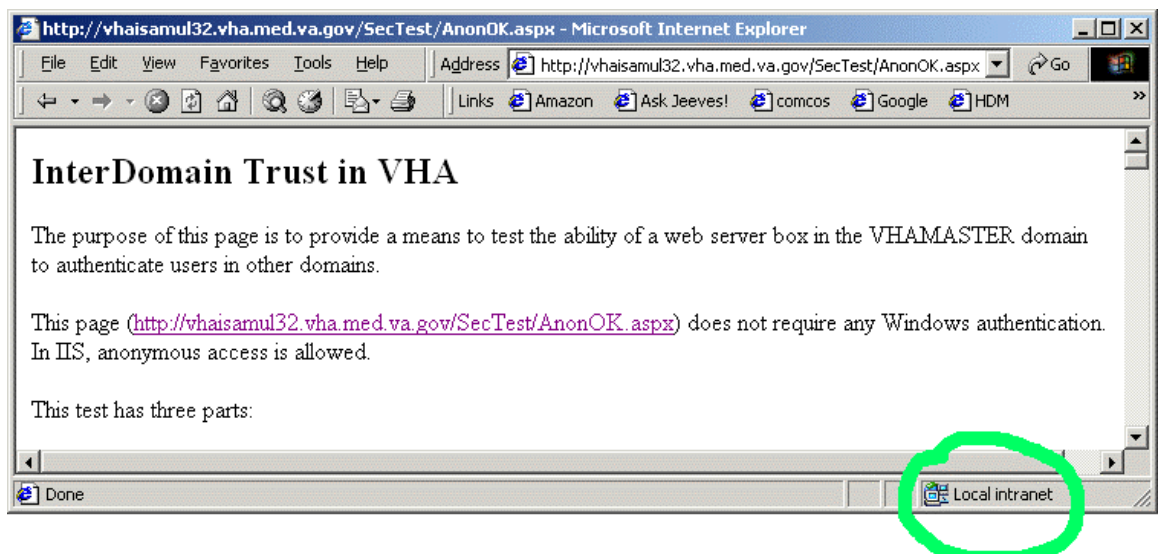


5. In the "Add this Web Site to the Zone" box, enter "*.va.gov" and press the Add button. The dialog box will look like this:

Browser Setup Instructions



6. Keep clicking OK to save these changes and exit out to your browser window.
7. Check that the Security Zone, located in the lower right-hand portion of Internet Explorer's status bar, now shows "Local intranet" when you access any site ending in "...med.va.gov":



If your browser shows "...med.va.gov" pages as "Local intranet" zone, your browser is ready.

Auto-Login Kiosk Setup Instructions

Overview

The auto-login kiosk allows volunteers to login into the Voluntary Services System, post their time for the day, and print a meal ticket. This section is a detailed instructional guide for the IRM staff to use to properly install an auto-login Kiosk station.

For the auto-login system to work properly, Windows 2000 operating system is required. The NT 4.0 operating system will not allow the left margins to view the first character on the meal ticket.

Due to technical issues at each facility, the auto-login instruction may change from time to time, therefore, we suggest that you refer to the VSS Web page at: <http://vista.med.va.gov/migration/vss>, for the latest version of this document.

It is strongly advised that the IRM allocate a resource for a total of two full days in the two-week period before data migration. It is crucial to the success of site implementation to set up, test, troubleshoot, and instruct staff on the use of the auto-login kiosks well in advance of data migration.

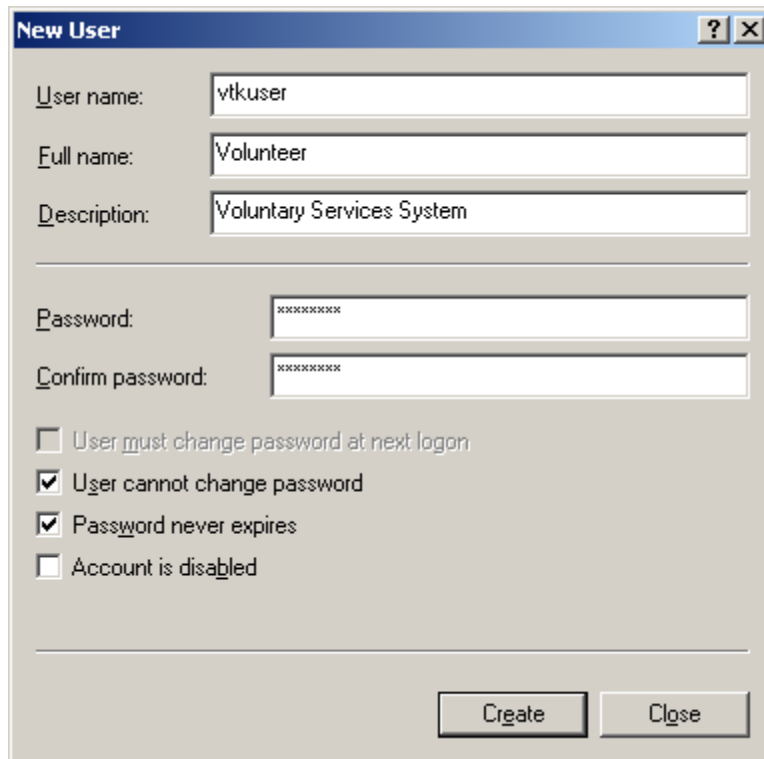
Before setting up the Kiosk, you will need to obtain the following from System Implementation:

- System Policy Editor (POLEDIT) zip file
- Station Number that corresponds to your site.

For the auto-login policy definitions, see *Appendix A* of this document.

Kiosk Setup Steps

1. Logon as an Administrator. Create a new local user account, *vtkuser*.
 - a. Open **Start | Settings | Control Panel**, followed by **Administrative Tools | Computer Management**
 - b. In the console tree, open **Local Users and Groups | Users**
 - c. Select **Action | New User...** and complete the **New User** dialog:



Choose a password for this account that complies with the organization's guidelines for secure passwords.

- d. Logon using the new *vtkuser* user account. The correct account is **<XXX (this computer)\vtkuser>**
- e. Disable the Quick Launch bar. Right-click an empty area on the taskbar, click **Toolbars**, and then click (uncheck) **Quick Launch**.
- f. Logoff.
- g. Logon as an Administrator. Delete all items from *vtkuser's* Start Menu (i.e. all items in **C:\Documents and Settings\vtkuser\Start Menu\Programs**). Please note, if your machine has been upgraded from Windows NT to Windows2000, use the following path: **C:\WINNT\Profiles\vtkuser\StartMenu\Programs**.
- h. Logoff.

Auto-Login Kiosk Setup Instructions

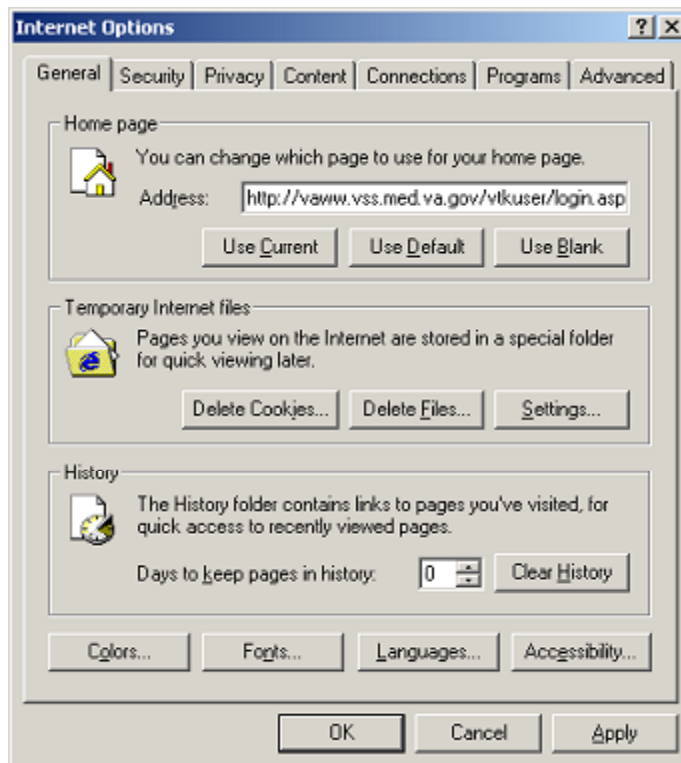
2. Logon as **vtkuser**. Launch Internet Explorer and configure the browser.
 - a. Setup the Home page. Each site has a corresponding Station Number assigned to it and this value should be appended to the default URL (as an argument to the default page, login.aspx) to obtain the appropriate home page URL for a given site (please contact VSS Support for specific Station Number information),

<<http://vaww.vss.med.va.gov/vtkuser/>>

Example: Palo Alto (Station 640) uses the following URL,

<<http://vaww.vss.med.va.gov/vtkuser/login.aspx?StationNumber=640>>

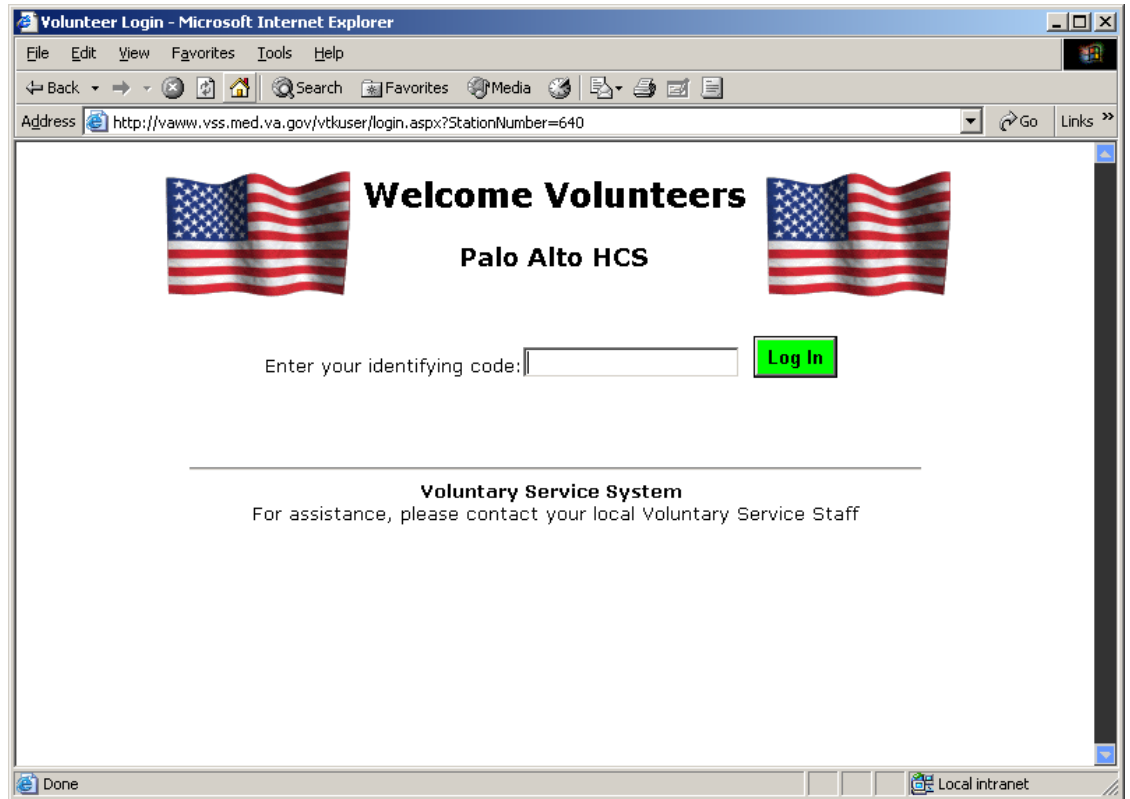
Open **Tools** | **Internet Options** and complete the dialog:



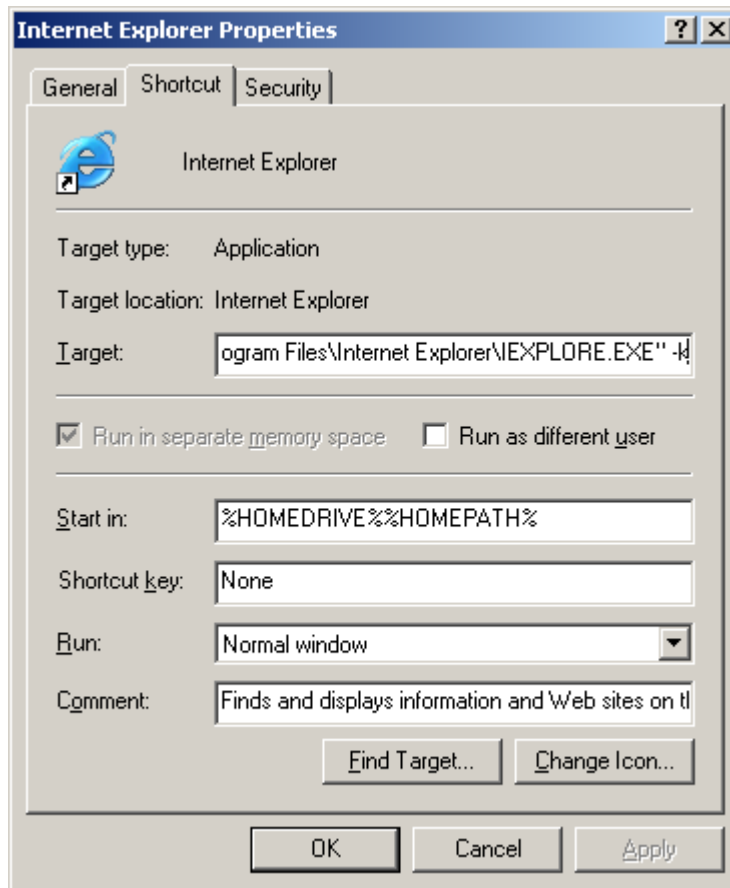
Note that the **Days to keep pages in history** setting is **0**.

- b. Verify browser operation and access to the VSS application with the new settings.

Auto-Login Kiosk Setup Instructions



- c. Logoff. Logon again (as *vtkuser*) and confirm that the settings remain in effect.
3. Logon as an Administrator. Create a shortcut to Internet Explorer to run in “kiosk mode”
 - a. Right-Click and Drag the Internet Explorer icon on the Quick Launch Bar to the desktop; select **Create Shortcut(s) here**.
 - b. Append a “-k” (space, dash k) to the program path (e.g. "*C:\Program Files\Internet Explorer\IEEXPLORE.EXE*" -k).

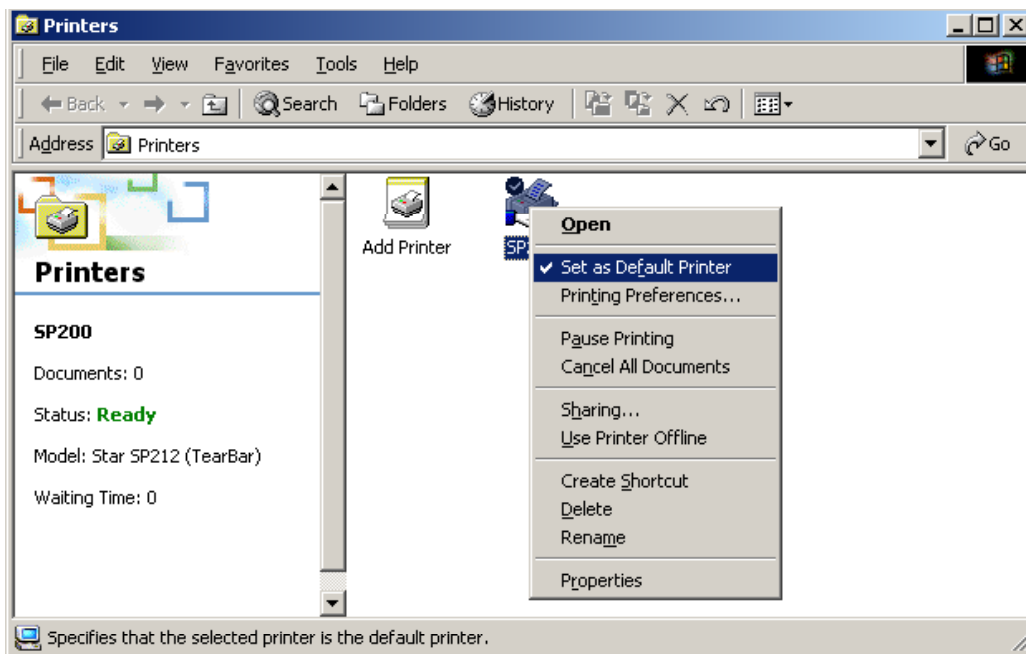


Note: It is essential that a space character be inserted before the “-k” (dash k) for the shortcut to work.

- c. Copy this shortcut to the **Startup** folder (... \Start Menu\Programs) in the **All Users** profile (e.g. C:\Documents and Settings\All Users\Start Menu\Programs\Startup).
- d. Logon as **vtkuser** and verify that Internet Explorer runs at startup. When run in Kiosk mode, the Internet Explorer title bar, menus, toolbars, and status bar are not displayed and Internet Explorer runs in Full Screen mode.

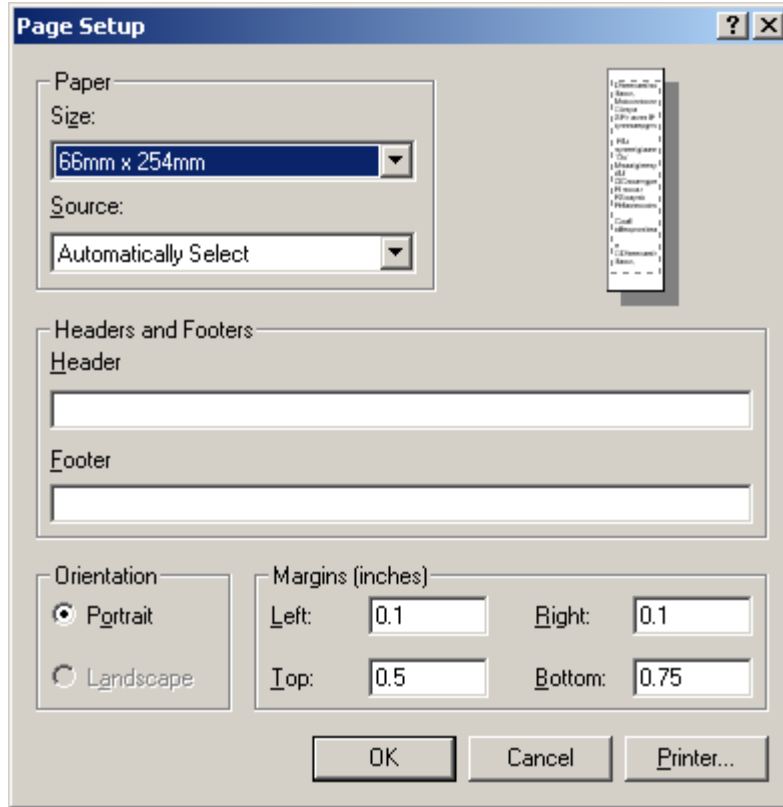
Auto-Login Kiosk Setup Instructions

4. Setup the default printer. These instructions will use a local Star Micronics SP200/SP212 line-mode printer as an example.
 - a. Attach the printer to the auto-login workstation using the correct cable. This cable is a DB9F to DB25M custom serial printer cable and can be connected to the computer in only one way. COM1 is the preferred serial port.
 - b. Logon as an Administrator. Setup the printer locally using the most-current driver (i.e. **linemode_2k-xp_20020723.exe**, dated 1/27/2003 1:36 PM) and port and verify operation (i.e. print a test page).
 - c. Logon as **vtkuser** and set the SP200 printer as the default.



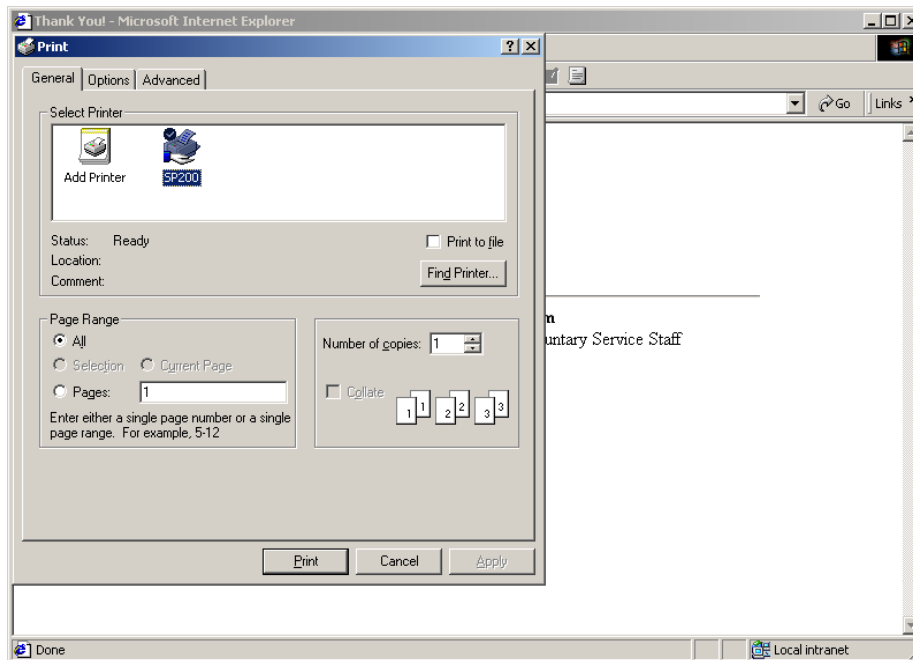
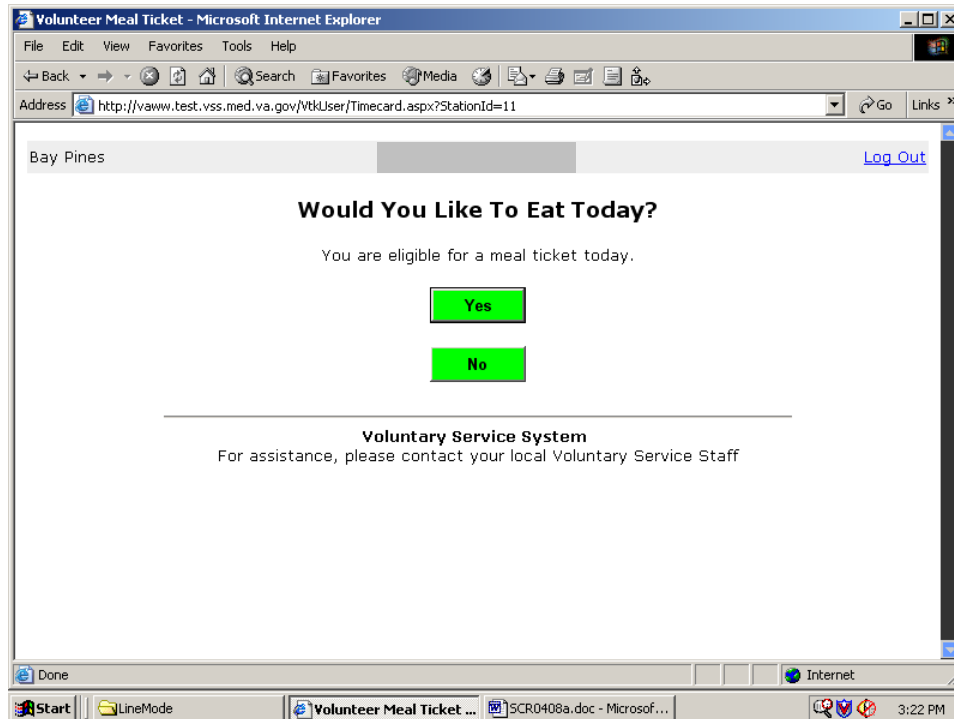
- d. Launch Internet Explorer and access the VSS Auto-Login application. Confirm the printer settings in **File | Page Setup:**
Paper Size – 66 x 254 mm; Margins: Left – 0.1, Right 0.1, Top – 0.5, Bottom – 0.75; no header or footer.

Auto-Login Kiosk Setup Instructions



- d. Generate a meal ticket using a valid volunteer ID, and verify printing. To obtain volunteer IDs, run the **Voluntary Sign-In Code** report for your station from within the main Voluntary Services System application (not the Auto-Login application).

Auto-Login Kiosk Setup Instructions



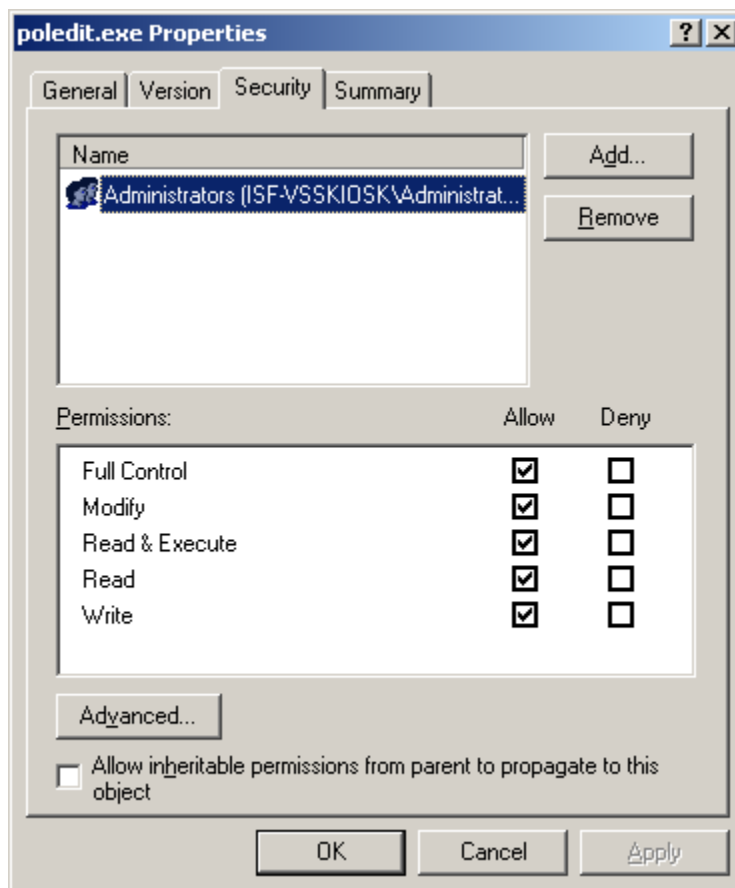
5. Logon as an Administrator. Install the System Policy Editor (POLEDIT) on the workstation, from the included zip file.

Auto-Login Kiosk Setup Instructions

- a. Extract the contents of the zip file to a temporary folder.
- b. Copy the extracted files. The following table lists the files that you need and the location to which they must be copied. *Note:* %SystemRoot% is typically C:\WINNT; the IEAK folder will need to be created.

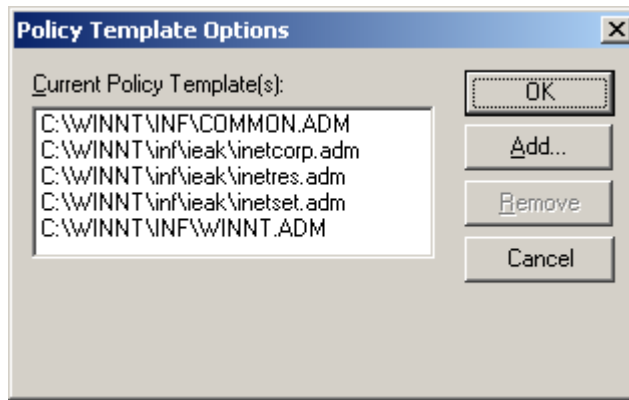
File name	Location
Poedit.exe	%SystemRoot%
Common.adm	%SystemRoot%\Inf
Winnt.adm	%SystemRoot%\Inf
Poedit.chm	%SystemRoot%\Help
Inetcorp.adm	%SystemRoot%\Inf\IEAK
Inetres.adm	%SystemRoot%\Inf\IEAK
Inetset.adm	%SystemRoot%\Inf\IEAK

- c. Protect access to the Poedit.exe file. Limit access to only Administrators (after clearing the **Allow inheritable permissions...** box, choose **Copy...** to permit subsequent deletion of the other names).



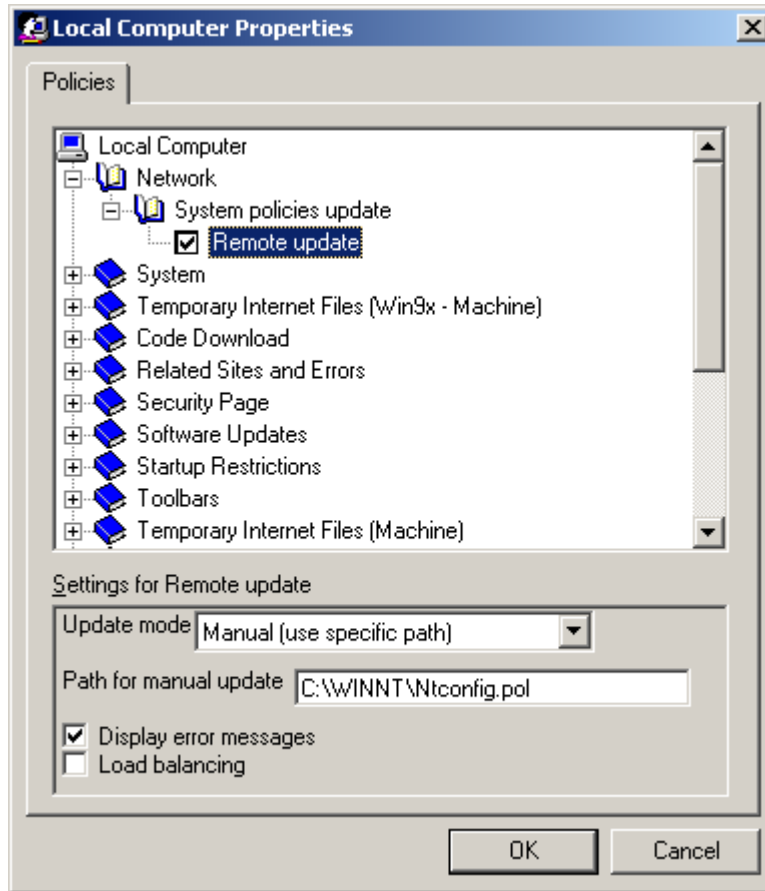
6. Attach the IEAK Policy Templates to System Policy Editor.

- a. Run **Poledit.exe**.
- b. With no policy open, select **Options | Policy Template**.
- c. Click **Add...** and add the **inetcorp**, **inetres** and **inetset** templates:



Templates attached in this manner add their policies to the policy properties dialog; once a template is attached, its policies are available whenever one creates new policies or views/edits existing policies.

- d. Exit the System Policy Editor.
7. Install the Policy file and configure the workstation to load this file from the local drive (the default is from a domain controller on the network).
- a. Copy the policy file, **Ntconfig.pol** from the included zip file to %SystemRoot% (e.g. C:\WINNT). Give this file the **Hidden** attribute.
 - b. Run **Poledit.exe**. Select **File | Open Registry** and open **Local Computer**.
 - c. Expand **Network | System Policies Update**.
 - d. Configure **Remote Update** as in the dialog below. (Confirm that **Remote Update** is checked):



- e. Exit the System Policy Editor, responding **Yes** to the “Do you want to save changes to the Registry?” dialog.
 - f. Login as **vtkuser** and verify the policy is in effect. One indication of this is the use of the standard (Teal) Windows background. Look for this background change during the login process before Internet Explorer runs.
8. Logon as an Administrator. Further restrict the Start Menu and Taskbar. Using Group Policy (**i.e. Start | Run | gpedit.msc**), enable the following policies:
- Local Computer Policy | User Configuration | Administrative Templates | Start Menu & Taskbar:
- Remove common program groups from Start Menu**
 - Remove Documents menu from Start Menu**
 - Remove Help menu from Start Menu**
 - Disable drag-and-drop context menus on the Start Menu**
 - Disable changes to Taskbar and Start Menu Settings**
 - Disable context menus for the taskbar**
9. Further restrict Internet Explorer. Using Group Policy (**i.e. Start | Run | gpedit.msc**), enable the following policies:

- a. Local Computer Policy | User Configuration | Administrative Templates | Windows Components | Internet Explorer:
Search: Disable Search Customization
Search: Disable Find Files via F3 within the browser
- b. Local Computer Policy | User Configuration | Administrative Templates | Windows Components | Internet Explorer | Browser Menus:
Disable Context Menu
Disable Open in New Window menu option
- c. Disable Internet Explorer's help. Rename **ieexplore.chm** located in C:\WINNT\Help.

10. Further restrict Internet Explorer's Search function.

- a. Using Notepad, create a text file with the following content: "Search is disabled".
- b. Save this to **C:\WINNT\nosearch.txt**. Give this file **Read-Only** and **Hidden** attributes.
- c. Add the following String Values (REG_SZ) to the indicated Registry Key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Search
SearchAssistant=C:\WINNT\nosearch.txt
CustomizeSearch=C:\WINNT\nosearch.txt

11. Restrict access to local drives. Using Group Policy (i.e. **Start | Run | gpedit.msc**), enable the following policy:

Local Computer Policy | User Configuration | Administrative Templates | Windows Components | Windows Explorer:
Prevent access to drives from My Computer

12. Login as **vtkuser** and confirm that the application runs as intended with the implemented restrictions in effect.

Troubleshooting

The user policy is by design very restrictive. It is not possible to make even the smallest environment change when logged in as the local user. Use a local administrator account for this purpose – e.g., to change the Page Setup setting in Internet Explorer.

If you are not able to make a change as a local user, the only alternative is to delete the local user account, recreate it (it can have the same name), and redo the setup steps listed above." Therefore you should finalize any environmental settings before applying the policy (steps 2 through 7).

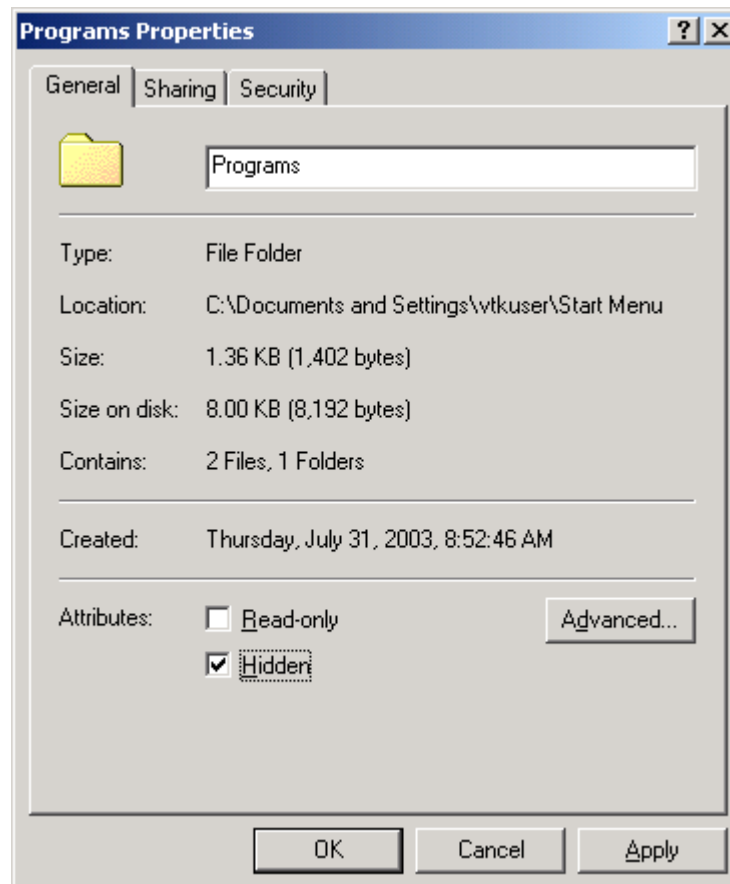
Installing Windows Patches

When Service Pack 4 for Windows 2000 is installed, shortcuts for Internet Explorer and Outlook Express may be added to the Start Menu and Quick Launch Bar of the kiosk PC. This means that volunteers will have access to Internet Explorer and Outlook Express through the Kiosk, which is contrary to VSS policy. Volunteers should not be able to use the kiosk for any purpose except recording hours and requesting meals.

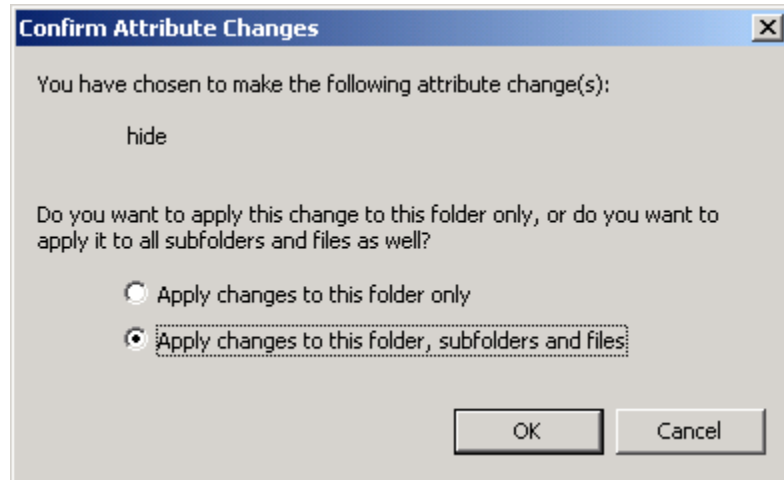
There are two ways that a person with administrative rights can resolve the problem:

- If Service Pack 4 *has already been installed*, log on as local administrator and delete the shortcuts before returning the kiosk PC to operation.
- If Service Pack 4 *has not yet been installed*, log on as local administrator and modify the attributes of the Start Menu so that the installer cannot create the shortcuts:

1. Add **Hidden Attributes** to the folder **C:\Documents and Settings\vtkuser\Start Menu\Programs**.



2. When you apply this change, you will also need to select **Apply changes to the folder, subfolders, and files**.



Data Migration Instructions

Data migration is the process of moving data from local Voluntary databases, used by the VTK system, to the national Voluntary Service System (VSS) database, used by the new VSS application. For each Voluntary site, the migration process takes place in two phases:

1. Data cleansing
2. Data transmission

Each of the phases involves the use of a software patch, which is distributed to the site IRM by SI. The data cleansing patch is referred to as Patch 33 (ABSV*4.0*31) and the data transmission patch as Patch 32 (ABSV*4.0*32). IRM will install both patches. An appointed Voluntary Services staff person will run both of them.

This section presents background information and instructions for installing and using Patches 33 and 32. It is divided into the following subsections: Data Cleansing (Patch 31) and Data Transmission (Patch 32). Each subsection is divided into introductory material, IRM installation instructions, and Voluntary instructions for running the program.

Data Cleansing

Patch 31 allows a Voluntary station to do the following:

- Send station information to the EMC that they will use to set up the station in the new VSS application
- Check existing VTK data for errors, redundancies, and inconsistencies
- Print error reports so that Voluntary can fix the errors prior to transmitting the data to the EMC.

IRM Installation Instructions

IRM is responsible for *installing* the Data Cleansing Patch. The following information pertains to the installation:

- The patch should take less than 1 minute to load
- No existing data is changed during patch installation
- No options need to be disabled
- None of these routines are or will be mapped
- Users can be on the system when this patch loads.

Follow the steps below to install Patch 33:

1. Use the 'INSTALL/CHECK MESSAGE' option on the PackMan menu. This option will load the KIDS package onto your system.
2. From the Kernel Installation and Distribution System (KIDS) menu, you may elect to use the following options:
 - a. Verify Checksums in Transport Global - this option will allow you to ensure the integrity of the routines that are in the transport global.
 - b. Print Transport Global - this option will allow you to view the components of the KIDS build.
 - c. Backup a Transport Global - this option doesn't need to be run because all of the routines in this patch are new.
 - d. Compare Transport Global to Current System - this option doesn't need to be run because all components in this patch are new.
3. Use the Install Package(s) option and select the package ABSV*4.0*33.
4. When prompted 'Want KIDS to Rebuild Menu Trees Upon Completion of Install? YES//', respond NO.
5. When prompted 'Want KIDS to INHIBIT LOGONs during the Install? YES//', respond NO.
6. When prompted 'Want to DISABLE Scheduled Options, Menu Options, and Protocols? YES//', respond NO.

Voluntary Data Cleansing Instructions

After patch 31 is installed at a site, the Voluntary Service staff can begin the data cleansing process. The cleansing process will start as soon as the patch is received by the site. It should be completed not later than two weeks before the sites scheduled conversion date.

Patch 31 installs a new menu on the Volunteer Timekeeping Activity menu, called the Voluntary Data Migration Menu. This menu is locked with the already existing ABSV MGR Security Key, so that only holders of that key will be able to run the menu options. These options are performed more or less in the order they appear in on the menu.

Voluntary Data Migration Menu		
Option	Purpose	Explanation
PREP	Prepare for Transition to VSS	PREP option does some initial setup for your site and sends information that is used to establish your site on the VSS centralized server. Run this option once only.
VAL	Validate Existing Data	VAL option checks your existing data and creates a report of entries that contain inconsistent data that can be corrected before the data is sent to the new system. This option can be run as often as you like.
PRNT	Print Results of Data	PRNT option displays the results of the Validate option. It

Data Migration Instructions

	Validation	can be run as often as you like.
VOL	Master Volunteer Edit	VOL option allows the user to edit all the fields they need to correct a problem with the Volunteer information.
DAIL	Daily Time Edit	DAIL option allows the user to edit all the fields they need to correct a problem with Regular Hours information.
OCC	Occasional Hours Edit	OCC option allows the user to edit all the fields they need to correct a problem with Occasional Hours information.
SEND	Send Voluntary Data to VSS	SEND option sends the data to the new system. It should be run only once unless SI instructs you to run it again. The Send option is installed only after Patch32 is installed to migrate the data.

The major steps in the data cleansing process are as follows:

1. Prepare Transition to VSS (PREP option)
2. Validate Existing Data (VAL option)
3. Print Data Validation Results (PRNT option)
4. Correct Data Errors (VOL, DAIL, OCC options)
5. Repeat steps 2-4 until no errors show up on the reports

These steps are described in detail in the sections below.

1. Prepare for Transition to VSS

The VSS application will contain information about the site's Voluntary Service. If the site is multi-divisional, it will contain information about each division to which Volunteer Hours are recorded. Most of the information about the Voluntary Service and its staff will be entered by Voluntary Service personnel using the new VSS web interface. However, some data is needed for initial setup of the site.

When you complete the PREP option, the EMC will have the data it needs to create your site in the VSS system. SI will contact you after your site has been initialized on VSS and the new system is ready to receive your data (Patch 32). SI will supply the e-mail address to use when running the option.

1. Select the PREP option.
2. The first seven questions are self-explanatory.
3. The questions about the User Administrator refer to the lead person at your site. That person will be responsible for entering site data and setting up other local users. Often, it will be the Voluntary Service Chief.

It is very important that this person's NT Username is entered correctly. You must enter both the domain and the username separated by a "\".

4. Enter an e-mail address for the recipient of this information. The message is sent via MailMan to a Microsoft Exchange address. SI will provide you with the necessary e-mail address. Your IRM must test that mail can be sent to the med.va.gov domain.

Sending this message will also test that domain, which will also be used when the actual data is sent. You can also send the message to local MailMan recipients.

2. Validate Existing Data

The data validation process will review all of the entries that will be moved from the VistA VTK system to the new VSS server during the migration. A report will be made containing each entry that has incorrect or inconsistent data. You can use that report to correct entries so that a complete set of data is moved to the new system.

Entries that are reported as problems will not be migrated to the new system until the problem is corrected in the VTK data. Because there are many records involved, running this option may take some time. Particularly time consuming will be the validation of the Volunteer Regular Hours.

When you run the VAL option, a dialog indicates the progress of the validation. When the check of each file is done, the number of entries with errors is displayed. After the validation finishes, you can immediately print the results. Whether you print it at this time or not, the information on incorrect entries is stored and can be printed at any later time.

The error reports are grouped by type and indicate the record number (IEN) of the record that contains the problem. For the volunteers, the name of the volunteer is also shown to help in identification.

The data validation option (VAL) can be rerun the status of your error correction efforts. You do not, however, need to rerun the option just to view the results of a prior run. You can print previous results.

3. Print Data Validation Results

You can print results of the Examination of Existing Data by selecting the PRINT option. The validation results are stored by date and time run. The simplest way to choose the results to print is to input the date that the validation was run.

In the following example, the results of validation run "TODAY" are requested. You select the specific set of data validated to print. In this example, the results for Regular and Occasional Hours are selected.

To print the results of the data validation:

Data Migration Instructions

1. Select the PRNT option from the VTK Data Migration menu. A list of the data validations performed appears.

```
Select VALIDATION RESULTS TIME RUN: TODAY OCT 04, 2002
  1 10-4-2002@18:14:10 Organizations NO, ONLY VALIDATION DONE
  2 10-4-2002@18:14:11 Services NO, ONLY VALIDATION DONE
  3 10-4-2002@18:14:11 Occasional Hours NO, ONLY VALIDATION DONE
  4 10-4-2002@18:14:11 Regular Hours NO, ONLY VALIDATION DONE
  5 10-4-2002@18:14:23 Volunteers NO, ONLY VALIDATION DONE
CHOOSE 1-5: 4 10-4-2002@18:14:11 Regular Hours NO, ONLY VALIDATION
DONE
```

The line “NO, ONLY VALIDATION DONE” means that the data was validated but not transmitted.”

2. In the top line, after “Select VALIDATION RESULTS TIME RUN:” enter “TODAY,” for today’s validation, or the date (in any form) that the validation was run.
3. In the bottom line, after “CHOOSE 1-5:” enter the number of one of the five reports that you want to view.
4. Enter “Yes” to the following print prompt:

Do you want to select another result to print?

The specified report prints and another Validation Results list appears on the screen.

5. Follow steps 2-4 above to print another report. If you do not want to print a report, enter “No” to the print prompt.

4. Correct Data Errors

You are requested to run the data validation option weeks before the actual switch to the new system so that you have the opportunity to correct invalid records. Corrected records will be migrated to the new system while those remaining with an error will be rejected.

The method of correction will depend on the problem. In some cases, you will have to contact volunteers for the information; in others, you will have to refer to paper records. When the necessary information is obtained, you will usually be able to use the existing VTK options to make the change. You can also use the three options supplied in this patch: Master Volunteer Edit, Daily Time Edit, and Occasional Hours Edit. If you cannot use the normal options, contact your local IRM. If your local IRM cannot resolve the issue they should file a NOIS report, and NVS will assist in getting the problem resolved.

Error Correction Example:

Volunteer record #3418 with Name MAYO,MARION has incorrect sex data.

Data Migration Instructions

This error means that a volunteer with record number 3418 in the Voluntary Master file, whose name is Marion Mayo, has incorrect information in the SEX field. It is unimportant how that erroneous data got there. If you determined that Marion was a woman, you would correct the error by using the Register/Edit Volunteer in the Master File option, as follows:

Select Master File Maintenance Menu Option: Register/Edit Volunteer in Master File

Select Volunteer Name: `3418 MAYO,MARION

Select the volunteer by putting an accent grave (`) in front of the entry number from the error report. This method should work for any data you are correcting, regardless of file. In this case, you could have also used the name.

Do you wish to Add/Edit Volunteer specific data? YES//<RET> (YES)

NICKNAME: <RET>
PSEUDO INDICATOR: <RET>
SOCIAL SECURITY NUMBER: 999-99-9999// <RET>
STREET ADDRESS #1: 1 Main St.// <RET>
STREET ADDRESS #2: <RET>
CITY: MORENO VALLEY// <RET>
STATE: CALIFORNIA// <RET>
ZIP CODE: 92553// <RET>

Here the source of the error is clear. Somehow a "Z" was input into the SEX field. The data validation option identified this as being incorrect. This particular error is corrected by changing the "Z" to an "F" for Female.

SEX: Z// F Female, 21 and over
BIRTH DATE: JUL 1970// ^
Do you wish to continue to the next section? YES// NO (NO)
Do you need to transmit this record to Austin? YES// NO (NO)
< No Action Taken>

Now, Marion's entry and the entries of the Regular Hours that she worked can be sent to the new system.

5. Repeat Validation and Correction (steps 2-4)

The validation and correction steps can be run as many times as necessary. Keep running them until all the errors listed in the report are gone. The data cannot be migrated with errors remaining.

Data Transmission

Patch 32 (ABSV*4.0*32) is used to send the corrected data to the EMC, where it becomes part of the national VSS database. It contains the SEND option, which appears on the VTK Data Migration menu. This option transmits the entire Voluntary site data to the EMC over the VA network, through a Microsoft Outlook e-mail message.

The IRM runs Patch 32. After Voluntary has corrected all the database errors located by Patch 31, SI will send the IRM Patch 32. When SI notifies the IRM through e-mail that the new system is prepared to accept the site's data, you can proceed to use the SEND option to transmit the data. Only one person at the site should run this option.

SI will provide the IRM with the e-mail addresses for sending the data. This may include a local mail address for possible troubleshooting purposes. The addresses used for the test run will not be the same as the go-live, production database run.

The export of local data will take place without user intervention. The program will tell you how many records were not sent because of errors, and allow you to print the errors. SI will inform IRM and Voluntary when the data has been received and stored into the new system. It will also inform you when Voluntary should start using the new, web-based Voluntary Service System.

Two Transmissions: Test and Production

There are two iterations of data transmission. The first will occur during the two weeks prior to actual migration ("go-live") date. This will be a practice run: the data will go to a test database at the EMC. The EMC may notify you of errors and ask the IRM to correct them (with SI's assistance) before resending the data.

The second iteration will be on the go-live date. This time the transmitted data will go into the production database. During the production iteration, the IRM will disable all the other VTK Data Migration menu options (PREP, VAL, PRNT, etc.) out of service before transmitting with the SEND option. It should also disable the auto-login kiosk. During data transmission Volunteer staff should log hours manually and supply the canteen with a list of volunteers entitled to receive a meal.

IRM Data Transmission Instructions

When Patch 32 is received from SI, the IRM should follow the steps below:

1. Install Patch 32 for Voluntary Services
2. Disable the auto-login Kiosk (production iteration only).
3. Check the following parameters:
 - In the MailMan Site Parameters, make sure that the NETWORK - MAX LINES SEND field is set to null

Data Migration Instructions

- In the Device file, make sure that the QUEUING field is **not** set to FORCED.

Here is a sample dialog for setting these two parameters (user input in bold):

Select Systems Manager Menu Option: **Manage Mailman**

Select Manage Mailman Option: **MailMan Site Parameters**

Select MAILMAN SITE PARAMETERS DOMAIN NAME:

OAKLAND.MED.VA.GOV

TIME ZONE: PST// **^NETWORK**

1 NETWORK - BLOCK SIZE RECEIVE

2 NETWORK - MAX LINES RECEIVE

3 NETWORK - MAX LINES SEND

CHOOSE 1-3: **3 NETWORK - MAX LINES SEND**

NETWORK - MAX LINES SEND: **<must be null>**

NETWORK - MAX LINES RECEIVE: **^**

Select MAILMAN SITE PARAMETERS DOMAIN NAME:

Select Systems Manager Menu Option: **Device Management**

Select Device Management Option: **Device Edit**

Select DEVICE NAME: **HFS** HOST DISK FILE TMP.TMP

NAME: HFS// **^QUEUING**

QUEUING: **<null or QUEUING ALLOWED or NOT ALLOWED>**

OUT-OF-SERVICE DATE: **^**

4. Disable all VTK Data Migration menu options except SEND (production iteration only).
5. When notified by SI that transmission was successful, enable the auto-login kiosk (production iteration only).

Voluntary Data Transmission Instructions

After you have corrected all data errors, SI will provide you with instructions to obtain patch #32 that installs the Send option on your system. When SI tells you that the new system is prepared to accept your data, you can proceed to send it. Only one person should be given the ABSV MIGRATION security key to run this option.

When directed to send data by SI, follow the steps below:

1. Select SEND option from the Voluntary Data Migration menu in VTK application.
2. When prompted, enter the e-mail addresses supplied by SI.
3. Print any errors reported by the program.
4. Report immediately to SI any problems that occur during the migration process.
5. Wait to receive one of the following notifications from SI:
 - There are problems with the data or transmission that need to be fixed

Data Migration Instructions

- That the transmission was successful, the site was created, and Voluntary should begin using the VSS application.

Appendix A: VSS RASIC Chart

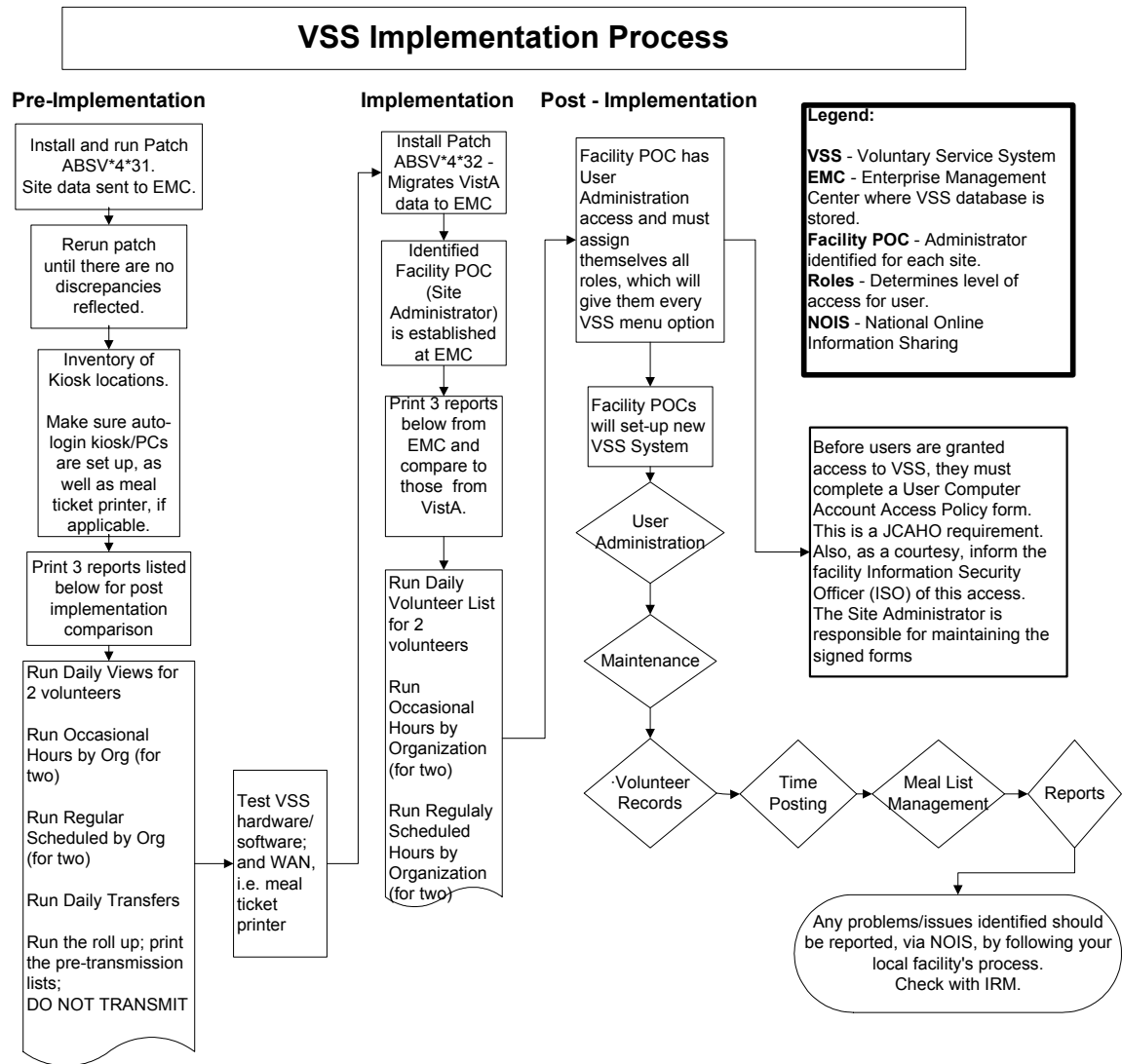
Activities	Project Participants									
	Migration Project Director	EMC Web Ops Director	VSS PM	SI Project Coord	NVS	EMC System Admin	VMS System Admin	VSS Team Members	QA Manager	SI Team Members
Establish project Start-Up team.	A	S	R	S	S	S	S	S	S	S
Create Timeline	A	S	R	S	S	S	S	S	S	S
Obtain Hardware Quote /Purchase Hardware	A	R	I			C	C			
Determine Configuration and Software Setup	A	A	S	S	S	R	C	I	I	I
Document the Agreement between EMC and VSS	A	A	R	I	I	S	S	C	I	I
Set up production and testing environment.	A	A	I	I	S	R	C	C	S	S
Establish change management process.	A	R	S	S	I	S	C	C	S	I
Update Security Patches	A	A	S	I	I	S	R	S	I	I
Determine financial procedures.	A	R								
Identify project risk.	A	A	R	S	I	C	S	C	I	I
Announce project.	A	I	I	R	I	I	I	I	I	I
Devise Backup procedures/Disaster Recovery	A	A	S	I	I	R	C	C	I	S
Devise Rollout Schedule	I	I	C	A	S	I	I	I	I	R
Determine Business process for data conversion, patch installation, data cleansing	A	I	S	R	R	S	S	S	I	S
Determine IV&V requirements for release	A	I	S	S	S	I	C	C	R	S
Release Product	S	S	S	S	R	S	S	S	C	S
Determine Capacity Management	I	I	C	C	S	R	C	C	S	C
Communicate with VDSI CM	A	I	R			C	C	S	I	

RASIC Chart Key

A RASIC Chart shows the responsibilities for individuals or roles for a variety of common activities that occur throughout the life of a project. Each RASIC code and a complete description is indicated below.

Code	Role Summary Description	Role Detail Description
R	Responsible for the process	Individuals who are responsible and accountable for the results of the decision. It is the job of these people to make the decision. They gather, analyze, and assess the data surrounding the decision. They are accountable for implementation and have an obligation to prevent the action if they do not agree. This role is required and only one Responsibility role is allowed for each task.
A	Approves or accepts the deliverables from the process	Individuals who approve or sanction. Those in the Approve role have the ability to accept or reject a recommendation or decision made by the Responsible role, and then to ensure that the people, time, and money are available for implementation.
S	Supports steps in the production of the deliverables	Individuals who are support or resource people. They may be subject matter experts who provide information about issues which affect the quality of the decision. Acceptance of a decision requires the commitment of those in the Support role. Support roles may not prevent a decision, but they do have the right to challenge it.
I	Needs information about the status and content of the deliverables	Individuals who need to be informed. Those in this role have the least level of involvement in decision-making and are affected in a minor way. This role is required for stakeholders who at least need to be informed so that energy and behavior can be focused. They may not block decisions, but they are free to ask questions for clarity and to express opinions.
C	Provides consultation for inputs, information or contributory deliverables	Individuals who can and are willing to consult.

Appendix B: VSS Implementation Diagram



Appendix B: VSS Implementation Diagram

Appendix C: Auto-Login Policy Definitions

The following table lists the actual policy settings as implemented. Policy Editor defines three states of policy changes: set (checked), unset (cleared), and unchanged (grayed). In the table below all listed policies are set except those preceded by the “!” character which represents “Not” (unset, cleared). All other settings are unchanged, “N/C”. To view or edit these settings, run POLEDIT, confirm the templates are loaded (item 6 above) and open the policy file C:\WINNT\Ntconfig.pol.

Each user policy has a properties dialog, which displays all categories, policies, and parts for that user policy. You can open the properties dialog for a policy in two ways: you can double-click the icon corresponding to the user policy you want to edit (i.e. vtkuser), or you can select it with the mouse and use the **Edit | Properties...** command.

The upper part of the properties dialog shows a tree view of the categories within the active user policy. When you first open a user policy, the categories all are collapsed; you can expand or collapse individual items by clicking the small +/- icon next to the category's name.

As you expand categories, you'll see checkboxes appear beneath them. Unlike normal Windows checkbox controls, these checkboxes can have three states:

- When checked, the policy is set (active), and its settings will be applied to turn on the policy when appropriate.
- When cleared, the policy is unset (inactive). Its settings will be applied to turn off the policy.
- When unchecked and gray, the policy is unchanged (inert). No changes will be made to a policy or its parts when its checkbox is grayed.

You must pay careful attention to the wording of the policy to make sure that the effect is what you intend. For example when the checkbox next to “Disable Registry editing tools” is checked, the tools are disabled. When it's cleared, the tools are not disabled, and when it's unchecked and gray, the settings currently in effect on each target machine, group, or user remain intact.

As you select individual policies within a category, notice that the contents of the settings area at the bottom of the properties dialog change. Some policies can have multiple parts; for example, the “Restrict display” policy has a total of five parts. You can set the value of each part independently of the others. Parts may accept on/off, numeric, or list selection choices, depending on what the policy template specifies.

You can move through the properties dialog, making changes as you go. POLEDIT preserves the changes within the current editing session, but they'll be lost unless you save the policy file.

POLICY DEFINITIONS FOR: *vtkuser*

(Implemented by templates from the Internet Explorer Administration Kit, IEAK)

Temporary Internet Files (NT4/Win2000 - User)

N/C

Internet Property Pages

Internet Property Pages

- Disable viewing the General Page
- Disable viewing the Security Page
- Disable viewing the Content Page
- Disable viewing the Connections Page
- Disable viewing the Programs Page
- Disable viewing the Advanced Page
- Disable changing any settings on the Advanced Page

General Page

General Page

- Disable changing home page settings
- Disable changing Temporary Internet files settings
- Disable changing history settings
- Disable changing color settings
- Disable changing link color settings
- Disable changing font settings
- Disable changing language settings
- Disable changing accessibility settings

Connections Page

Connections Page

- Disable Internet Connection Wizard
- Disable changing connection settings
- Disable changing proxy settings
- Disable changing Automatic Configuration settings

Content Page

Content Page

- Disable changing ratings settings
- Disable changing certificate settings
- Disable changing Profile Assistant settings
- Disable AutoComplete for forms and saving of submitted strings
- Do not allow users to save passwords in AutoComplete for forms

Programs Page

Programs Page

- Disable changing Messaging settings
- Disable changing Calendar and Contact settings

Appendix C: Auto-Login Policy Definitions

Disable the Reset Web Settings feature

Disable changing checking if Internet Explorer is the default browser

Appendix C: Auto-Login Policy Definitions

Browser Menus

File Menu

- Disable Save As... menu option
- Disable New Window option from File menu
- Disable Open menu option
- Disable Save As Web Page Complete format
- Disable closing of the browser
- !Disable printing from the browser

View Menu

- Disable Source menu option
- Disable Fullscreen menu option

Favorites Menu

- Hide Favorites Menu

Tools Menu

- Disable Internet Options... menu option

Help Menu

- Remove 'Tip of the Day' menu option
- Remove 'For Netscape Users' menu option
- Remove 'Tour' menu option
- Remove 'Send Feedback' menu option

Context Menu (right click)

- Disable Context Menu
- !Disable Open in New Window menu option

File Download Dialog

- Disable Save this program to disk option

Favorites and Search

Favorites Import/Export

- Disable importing and exporting of favorites

Search

- Disable Search Customization
- Disable Find Files via F3 within the browser

Persistence

N/C

Dial-Up Settings

N/C

Language Settings

Language Settings

- Default language for menus and dialogs: English

Temporary Internet Files (User)

N/C

Appendix C: Auto-Login Policy Definitions

Toolbars

Default Toolbar Buttons

Show small icons

Back button: Turn button off

Forward button: Turn button off

Stop button: Turn button off

Refresh button: Turn button off

Home button: Turn button off

Search button: Turn button off

History button: Turn button off

Favorites: Turn button off

Folders button: Turn button off

Fullscreen button: Turn button off

Tools button: Turn button off

Mail button: Turn button off

Font size button: Turn button off

Print button: Turn button on

Edit button: Turn button off

Discussions button: Turn button off

Cut button: Turn button off

Copy button: Turn button off

Paste button: Turn button off

Encoding button: Turn button off

Print preview button: Turn button off

Advanced Settings

Browsing

!Launch browser in full screen mode

AutoComplete

N/C

Display Settings

N/C

Appendix C: Auto-Login Policy Definitions

Advanced Settings

Browsing

- !Disable script debugging
- !Show friendly URLs
- Use smooth scrolling
- Enable page transitions
- Enable page hit counting
- !Automatically check for Internet Explorer updates
- Underline links: Always
- !Enable folder view for FTP sites
- !Show Go button in Address bar
- Show friendly http error messages
- !Display a notification about every script error
- All others N/C

URL Encoding

N/C

(Implemented by standard Windows templates)

Control Panel

Display

- Restrict display
 - Deny access to display icon
 - Hide Background tab
 - Hide Screen Saver tab
 - Hide Appearance tab
 - Hide Settings tab

Desktop

- !Wallpaper
- Color scheme
 - Scheme name: Windows Default

Shell

Restrictions

- Remove Run command from Start menu
- Remove folders from Settings on Start menu
- Remove Taskbar from Settings on Start menu
- Remove Find command from Start menu
- Hide drives in My Computer
- Hide Network Neighborhood
- No Entire Network in Network Neighborhood
- No workgroup contents in Network Neighborhood
- Hide all items on desktop
- Remove Shut Down command from Start menu
- Don't save settings at exit

Appendix C: Auto-Login Policy Definitions

Appendix C: Auto-Login Policy Definitions

System

Restrictions

- Disable Registry editing tools

- All others N/C

Windows NT Shell

Custom user interface

- N/C

Custom folders

- N/C

Restrictions

- Remove View->Options menu from Explorer

- Remove Tools->GoTo menu from Explorer

- Remove File menu from Explorer

- Remove common program groups from Start menu

- Disable context menus for the taskbar

- Disable Explorer's default context menu

- Remove the "Map Network Drive" and "Disconnect Network Drive" options

- Disable link file tracking

- Remove NT Security item from Start menu

- Remove Disconnect item from Start menu

- Prevent user from changing file type associations

- All others N/C

Windows NT System

- Disable Task Manager

- Disable Change Password

- !Show welcome tips at logon

- All others N/C

Windows NT User Profiles

- N/C